Experimental realization of a highly secure chaos communication under strong channel noise

Weiping Ye[1], Qionglin Dai[1], Shihong Wang[2], Huaping Lü[2], Jinyu Kuang[1], Zhenfeng Zhao[1], Xiangqing Zhu[1], Guoning Tang[2], Ronghuai Huang[1], ang Gang Hu[2,3,†]

[1] *Department of Electronics, Beijing Normal University, Beijing, 100875, China*

[2] *Department of Physics, Beijing Normal University, Beijing, 100875,China and*

[3] *The Key Laboratory of Beam Technology and Material*

[†] *Correspondent author (email:ganghu@bnu.edu.cn)*

(Dated: February 8, 2008)

Abstract

A one-way coupled spatiotemporally chaotic map lattice is used to contruct cryptosystem. With the combinatorial applications of both chaotic computations and conventional algebraic operations, our system has optimal cryptographic properties much better than the separative applications of known chaotic and conventional methods. We have realized experiments to pratice duplex voice secure communications in realistic Wired Public Switched Telephone Network by applying our chaotic system and the system of Advanced Encryption Standard (AES), respectively, for cryptography. Our system can work stably against strong channel noise when AES fails to work.

Keywords: Spatiotemporal chaos; Chaotic cryptography; Error function attack

PACS numbers: 05.45.Vx, 05.45.Ra, 43.72.+q

I. INTRODUCTION

Chaotic systems have several significant features favorable to secure communications, such as aperiodicity (useful for one-time pad cipher); sensitivity to initial condition and parameters (useful for effective bit confusion and diffusion [1]); and random-like behavior (useful for producing output with satisfactory statistics). With all these advantages scientists expected to introduce new and powerful tools of chaotic cryptography [2–7]. Nevertheless, during the last decade, many pitfalls and drawbacks of cryptosystems based on chaos synchronization have been found. The main problems are: low security due to easy reconstruction of chaotic dynamics [8–12], slow performance speed due to analytical floating-point computation, and weak resistance against channel noise due to large bit error propagation caused by finite chaos synchronization time. Recently, various methods have been suggested to solve the above problem [13–17]. In this paper we propose to use a one-way coupled chaotic map system to construct a cryptosystem with optimal overall properties. The crucial merits of this system are: on one hand we use spatiotemporal chaos to fully apply and develop the advantages of chaotic cryptography, and on the other hand we incorporate some simple algebraic operations in the conventional cryptography to overcome the disadvantages of analytical chaotic computations. With the combinative applications of chaotic and conventional methods our system has optimal cryptographic properties much better than the separative applications of chaotic and conventional methods known so far. We design an experiment set with embedded CPUs and use this set to practice duplex voice secure communications in realistic wired Public Switched Telephone Network, by applying our chaotic cryptosystem and the system of the Advanced Encryption Standard (AES) [18], respectively, for comparisons. Experimental and numerical results show that our system is considerably better than AES with both security and performance speed. Most significantly, our system can work stably against strong channel noise when AES fails to work.

II. SPATIOTEMPORAL CHAOTIC CRYPTOSYSTEM (STCC)

We take a one-way coupled map lattice for spatiotemporal-chaos-based cryptography, which has the encryption transformation as

$$\begin{aligned} x_{n+1}(j) &= (1-\varepsilon)f_j[x_n(j)] + \varepsilon f_j[x_n(j-1)], \\ f_j(x) &= (3.75 + a_j/4)x(1-x),\ \ a_j \in [0,1], \\ j &= 1, \cdots, m \\ x_n(0) &= D_n/2^9 + 0.1 \end{aligned} \tag{1a}$$

$$\begin{aligned} x_{n+1}(m+1) &= (1-\varepsilon)f[x_n(m+1)] + \varepsilon f[x_n(m)], \\ Q'_n &= [\mathrm{int}(x_n(m+1) \times 2^{52})] \mod 2^{32} \\ Q_n &= Sbox(Q'_n) \\ f(x) &= 4x(1-x), \quad z_n = Q_n/2^{32} \end{aligned} \tag{1b}$$

$$\begin{aligned} x_{n+1}(m+2) &= (1-\varepsilon)f_1[x_n(m+2)] + \varepsilon f_1(z_n), \\ x_{n+1}(j) &= (1-\varepsilon)f_{j-m-1}[x_n(j)] \\ &\quad + \varepsilon f_{j-m-1}[x_n(j-1)], \\ j &= m+3, \cdots, 2m+1 \end{aligned} \tag{1c}$$

$$\begin{aligned} x_{n+1}(j) &= (1-\varepsilon)f[x_n(j)] + \varepsilon f[x_n(j-1)], \\ j &= 2m+2, \cdots, 2m+2N \end{aligned} \tag{1d}$$

$$\begin{aligned} y_{n+1}(1,1) &= (1-\varepsilon)f[y_n(1,1)] + \varepsilon f[x_n(2m+2N)] \\ y_{n+1}(j_1,1) &= (1-\varepsilon)f[y_n(j_1,1)] \\ &\quad + \frac{\varepsilon}{2}\{f[y_n(j_1-1,1)] + f[x_n(2m+2j_1-1)]\} \\ y_{n+1}(1,j_2) &= (1-\varepsilon)f[y_n(1,j_2)] \\ &\quad + \frac{\varepsilon}{2}\{f[y_n(1,j_2-1)] + f[x_n(2m+2j_2-2)]\} \\ y_{n+1}(j_1,j_2) &= (1-\varepsilon)f[y_n(j_1,j_2)] \\ &\quad + \frac{\varepsilon}{2}\{f[y_n(j_1,j_2-1)] + f[y_n(j_1-1,j_2)]\} \\ j_1, j_2 &= 2, 3, \cdots, N \end{aligned} \tag{1e}$$

$$\begin{aligned}
K_n(j_1,j_2) &= \text{int}[y_n(j_1,j_2)\times 2^{52}] \mod 2^{32}, \\
S_n &= [K_n(j_1,j_2)+I_n(j_1,j_2)] \mod 2^{32}, \\
j_1,j_2 &= 1,2,\cdots,N \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (1f) \\
D_n &= [S_n(N,N) \gg 24]\&255
\end{aligned}$$

where the S-box is defined as

$$\begin{aligned}
A_1 &= [(Q'_n \gg 24)\&255], A_2 = [(Q'_n \gg 16)\&255], \\
A_3 &= [(Q'_n \gg 8)\&255], A_4 = [(Q'\&255], \\
A_0 &= A_1 \oplus A_2 \oplus A_3 \oplus A_4 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (2) \\
Q_n &= [A_0 \ll 24] + [A_4 \ll 16] + [A_3 \ll 8] + A_2
\end{aligned}$$

The operation $x \gg y$ ($x \ll y$) denotes a right (left) shift of x by y bits, the & operator is bitwise AND, and $\oplus$ means bitwise XOR.

The decryption system is driven by the transmitted signal as

$$x'_n(0) = D_n/2^9 + 0.1$$

and all other dynamic forms of the receiver are exactly the same as those of the transmitter with $x_n(j)$, z_n, $y_n(j_1,j_2)$, $K_n(j_1,j_2)$, $I_n(j_1,j_2)$, and $\mathbf{a}=(a_1,a_2,\cdots,a_m)$ replaced by $x'_n(j)$, z'_n, $y'_n(j_1,j_2)$, $K'_n(j_1,j_2)$, $I'_n(j_1,j_2)$, and $\mathbf{b}=(b_1,b_2,\cdots,b_m)$, respectively. With $\mathbf{b}=\mathbf{a}$, the receiver can reach chaos synchronization with the transmitter, and successfully recover the true plaintext as

$$\begin{aligned}
\mathbf{b} &= \mathbf{a}, \;\; y'_n(j_1,j_2) = y_n(j_1,j_2), \\
K'_n(j_1,j_2) &= K_n(j_1,j_2), \;\; I'_n(j_1,j_2) = I_n(j_1,j_2) \qquad\qquad\qquad\qquad\qquad\qquad\qquad (3)
\end{aligned}$$

In Eqs.(1)-(3) three parameters ε, m, N are adjustable for controlling different cryptographic properties of the system, according to the actual requirements of realistic secure communications. In this paper, we fix

$$\varepsilon = 0.99, \quad m = 3, \quad N = 4 \tag{4}$$

and will simply call our spatiotemporally chaotic cryptosystem Eq.(1) with parameters (4) as STCC. The scheme of STCC is shown in Fig.1, and the decryption system has exactly the same structure with feedback structure of the transmitter replaced by driving structure in the receiver. The former is thus a high-dimensional hyperchaos while the latter becomes nonchaotic with all conditional Lyapunov exponents negative.

The important and new point of system (1) is that we apply both floating-point analytical computation of spatiotemporal chaos and algebraic operations of integer numbers to construct our cryptosystem which possess the advantages of both chaotic and conventional cryptographies.

First, we use high-dimensional spatiotemporal chaos as the basic structure of the cryptography, which leads to the following significant advantages. (i) Due to the high-dimensionality and chaoticity, the output keystreams and ciphertexts have high complexity, long periodicity of computer realization of chaos, and effective bit confusion and diffusion in many directions in the variable space. All these properties are favorable to achieve high practical security [17]. (ii) Due to the extended nature of STCC we are able to use many sites ($N \times N = 16$ square sites in Fig.1) to produce keystreams in parallel and greatly increase the speed of performance [6]. (iii) With one-way coupled maps and strong coupling ($1 - \varepsilon \ll 1$), the receiver can easily reach chaos synchronization with the transmitter by a single driving D_n. Note, for each iteration the driving D_n has only 8 bits while the total ciphertext 512 bits. This separation of driving bits from nondriving ciphertext bits makes the communication well resistant against strong channel noise. This point will be the central focus later in our experiment.

After the above advantages of STCC, the following algebraic operations of Eq.(1) can further and greatly improve the cryptographic properties of the system. (i) In Eq.(1f) we apply an algebraic operation *int,* which makes all keystreams $K_n(j_1, j_2)$, ciphertext $S_n(j_1, j_2)$, and driving signal D_n integer numbers. These integralizations are extremely important for the robustness of highly secure communications against computer round-off errors and channel noise [14]. (ii) In Eqs.(1b) and (1f) we apply *modulo* operations [13, 16], which can considerably enhance the key sensitivity of the system, and can also effectively improve the random-like statistics of the transmitted signals. (iii) In Eqs.(1b) and (2) we incorporate a S-box algebraic operation [17], which makes any analytical solution aiming at exposing the secret key extremely difficult. All the algebraic operations (i)-(iii) have been popularly used in the conventional cryptography. These operations are so simple that they need very low computational expenses; and so weak that they cannot play significant role in the conventional cryptography by themselves. However, incorporating with the analytical computerization of STCC, these simple algebraic operations play important roles in optimizing the cryptographic properties of the system, because they are just suited, with very little cost, to overcome the weakness of chaotic cryptography mentioned in the introduction and allow the advantages of STCC fully developed.

III. CRYPTOGRAPHIC PROPERTIES OF STCC

We have evaluated various cryptographic properties of system (1). Specifically, we have analyzed in details its security, performance, and robustness, and compared these properties with those of AES. It is found that STCC is considerably better than AES in all the above essential aspects.

(A) Security

We have evaluated the security of STCC by trying various effective attacks based on key-sensitivity analysis; statistical-property analysis; and analytical-solution analysis with the conditions of public-structure and known plaintext, and find that no any tested method can be more effective than the brute force attack. The detail of these evaluations (in particular, the atatistics-based evaluations) will appear elsewhere [17]. In this paragraph we focus on the key sensitivity analysis by using the error function attack [16].

Since we consider public-structure and plaintext-known attacks, any intruder can run the receiver system with the test key $\mathbf{b}$ to produce $I'_n(j_1, j_2)$, and then compare the output $I'_n(j_1, j_2)$ with the true plaintext $I_n(j_1, j_2)$ for exposing the location of $\mathbf{a}$. Specifically, the intruder can compute the following error function

$$e(j_1, j_2; \mathbf{b}) = \frac{1}{T} \sum_{n=1}^{T} |i'_n(j_1, j_2) - i_n(j_1, j_2)| \tag{5}$$

$$i_n(j_1, j_2) = \frac{I_n(j_1, j_2)}{2^{32}}, \quad i'_n(j_1, j_2) = \frac{I'_n(j_1, j_2)}{2^{32}}$$

The secret key $\mathbf{a}$ can be extracted by minimizing the error function as

$$e(j_1, j_2; \mathbf{b}) = 0 \qquad \text{at} \quad \mathbf{b} = \mathbf{a} \tag{6}$$

This evaluation is called as the error function attack (EFA), which can be used to analyze the key sensitivity property of the system.

In Figs.2(a) and (b) we fix $b_2 = b_3 = a_1 = a_2 = a_3 = 0.5$ and plot $e(1, 1; b_1)$ vs b_1 with $T = 10^8$ for different detect resolutions. It is clearly shown that $e(1, 1; b_1)$ raises rapidly to $\frac{1}{3}$ with very small fluctuation for extremely small mismatch $|b_1 - a_1| \geq 2^{-45}$. The same behavior can be observed as well for b_2 and $b_{3.}$ In Fig.(2c) we fix $b_3 = a_3 = 0.5$ and plot $e(1, 1; b_1, b_2)$ vs b_1 and b_2, and observe a needle-like basin exactly at $b_1 = a_1, b_2 = a_2$. In Fig.2(d) we present the behavior of $e(1, 1; \mathbf{b})$ in the 3D parameter space. It is shown again that whenever $|\mathbf{b} - \mathbf{a}| \geq 2^{-45}$ in the 3D space, the error function raises immediately to about $\frac{1}{3}$. Therefore, the effective key number of our system against EFA is $(2^{45})^3 = 2^{135}$. It can be easily proven that two data sequences, completely uncorrelated and purely random and uniformly distributed in [0,1], have error value of Eq.(5) equal to $\frac{1}{3}$. The behavior of Figs.2(a)-(d) show convincingly excellent key-parameter-sensitivity and satisfactory random-like statistical properties. The cost for the intruder to break the security of our system by using EFA is quantitated as

$$Cost = 2^{135} \approx 10^{40} \tag{7}$$

which is also the cost of the brute force attack for the 2^{135} key number.

Chaotic system (1) has a significant advantages over AES with security. The security level of system (1) can be conveniently and greatly increased. Simply increasing m in Eq.(4) by one, we can surely enlarge the key number (i.e., the level of security) by 2^{45} times, with the cryptographic structure of Eq.(1) kept unchanging and with almost no increase (about 5% increase) of computational cost. Thus, the security of STCC is practically unshakable by the quick technology advance of attack machines, including possible future quantum computers. In comparison, in order to greatly increase the security level of AES, some other cryptographic properties have to be sacrificed in balance.

(B) Encryption (decryption) speed

Usually, the floating-point analytical computation of real variables used in chaotic cryptography is considerably slower than the algebraic operations of integer numbers used in conventional cryptography. The encryption speed of the former is thus often not comparable with that of the latter when the securities of both systems are comparable. Nevertheless, STCC has rather fast speed, because it fully takes the advantages of spatiotemporal chaos in performance. By keeping high security, STCC produces ciphers in every iteration (one-round encryption structure), and meanwhile in each iteration many [$4 \times 4 = 16$ for Eq.(4)] sites make encryption operations in parallel. Therefore, with software implementation our STCC has very high speed, higher than AES (which, with key of 128 bits, takes 10 rounds for producing ciphers of a block). Specifically our STCC can encrypt 914Mbit and 430Mbit per second with 2GHz (A) and 700MHz (B) CPU computers, respectively, while AES (with 128-bit key length and 128-bit block length) produces 267Mbit and 96Mbit ciphers for the same computers. STCC is therefore faster than AES for 3.4 and 4.4 times with computers A and B, respectively.

A crucial point for the validity of the parallel encryption operations in Fig.1 is that all the keystreams produced by the 16 square sites should be practically uncorrelated from each other. We checked this point and found that these keystreams are uncorrelated from each other and insuppressible indeed, and this validates the parallel encryptions of Eq.(1) and Fig.1.

(C) Robustness of communications against channel noise

With the extremely high sensitivity shown in Fig.2, the problem of robustness and reliability of secure communication against computer round-off errors and channel noise should be carefully examined. It is well known that all block-cipher systems and stream-cipher systems with self-synchronizing scheme have a problem of bit error propagation (or say, bit error avalanche), i.e., one bit error in the driving signal may cause a large number of error bits in the received plaintext. In this regard, STCC has some essential advantages. The most significant feature of our system is that among the ciphers of 512 bits produced in each iteration [$S_n(j_1, j_2), j_1, j_2 = 1, 2, 3, 4$] only 8 bits (D_n) are used for driving. Therefore, only $\frac{1}{64}$ transmitted bits (driving bits) have bit error avalanche problem, and all other bits (nondriving ciphertext bits) have not. Hence, in average the avalanche destruction can be considerably reduced in our case. In order to reduce the avalanche effect people must include some additional bits for protection of the driving signal, and this increases the cost of both cryptography and signal transmission. In doing so our STCC has a great advantage over

AES because in AES one should protect all transmitted bits (each error bit of the ciphertext has an equal error avalanche of 128 bits in the receiver plaintext) while for our system only the driving bits, i.e., 8 driving bits among the total 512 cipher bits, have the avalanche effect and need to be particularly protected. This advantage will be shown, in our following experiment, to be extremely important for the secure communications under strong channel noise.

IV. EXPERIMENTS AND COMPARISONS OF STCC AND AES

Now we come to the central part of the present paper: the experimental realization of STCC and the experimental comparisons between STCC and AES for robustness against channel noise. We have realized a duplex voice communication by using the Public Switched Telephone Network wired(PSTN). The scheme of the experimental set is presented in Fig.3, where the following significant points should be emphasized.

(i) In Fig.3 we use embedded CPUs connecting to other communication tools. These CPUs perform cryptographic operations as well as other communication tasks. Since the embedded CPU technique has been widely used in practical communications, the experimental set of Fig.3 is realistic for applications.

(ii) We use the realistic PSTN for practicing secure communications. Moreover, we intentionally add strong noise into the transmission channel to study the possibility of secure communications in wireless telephone systems where the channel noise is usually much stronger than the wired ones.

(iii) For the cryptographic part of the experimental secure communications, we apply both STCC and AES, respectively, for comparisons. In order to strengthen the resistance of the communications against channel noise, we add some additional bits in Channel Coding, for protecting the driving signals of both STCC and AES systems.

All the above arrangements are closely related to practice realistic secure communication service.

For the channel environment we assume additive white Gaussion noise, which yields certain fixed bit error rate (BER) of each transmitted bit. Therefore, we will directly vary error probability p of the transmitted signal bits to model the noise perturbation in the channel. Moreover, for the voice transmission from User A to User B we introduce BER before the part of "Modulation" of User A in Fig.3 rather than after "Modulation" in the channel, for the sake of convenience of experimental performances and measurements. This arrangement does not change any essence since we are interested only on the influence of different cryptographies not Modulation and Demodulation operations.

In the part of Channel Coding we apply the standard approach of bit-error correction [19]. In case of AES, for transmitting a block of 128 cipher bits we actually transmit 136 total bits, of which 8 additional noncipher bits are used for correcting one bit error among the all 136 transmitted bits[19]. The efficiency of the signal transmission is thus reduced by 6% (i.e., 6% transmitted bits do not contain plaintext information). This bit protection fails when two or more than two error bits appear in a single block of ciphertext. In case of STCC, we protect the driving bits D_n only, and leave other cipher bits $S_n(j_1, j_2)$ unprotected. For transmitting 512 ciphertext bits in each iteration, we add 20 additional bits to protect the 8 driving bits. This protection can correct maximum 5 error bits in 28 bits[19]. With this driving bit protection the efficiency of the signal transmission is reduced by about 4%.

Before the experiment of secure communication, we first examine the behaviors of normal nonsecure (without cryptography) communication (NNC) with various BER p's. The working qualities of NNC for different ranges of noise can be ranked subjectively and roughly by ears as: excellent for $p \lesssim \frac{1}{250}$; fairly well for $\frac{1}{250} < p \lesssim \frac{1}{100}$; bad for $\frac{1}{100} < p \lesssim \frac{1}{30}$; complete failure of voice communication for $p > \frac{1}{30}$. Therefore, we will compare the results of cryptographies of STCC and AES, in the range of p, $\frac{1}{2000} \leq p \leq \frac{1}{10}$.

In Fig.4(a) we plot p_N, p_S and p_A vs BER probability p without bit protection, where p_N, p_S and p_A are the bit error rates of NNC, STCC and AES secure communications, respectively. We have $p_N \approx p$ for all p values. This is reasonable since the "Modulation" and "Demodulation" functions in Fig.3 do not observably change the channel BER. Both p_S and p_A are much larger than p_N due to the error propagation effects (note, $p_{S,A} \approx 0.5$ implies/complete loss of the transmitted information). It is observed that p_S and p_A are in the same order. Without bit protection p_S is slightly larger than p_A, indicating that STCC has larger bit error propagation rate than that of AES.

In Fig.4(b) we do the same as Fig.4(a) except that p_S and p_A are measured with the function of bit error correction operating in Channel Coding and Decoding parts. With the designed bit protections both p_S and p_A become considerably smaller than those in Fig.4(a). For STCC it is striking that the bit errors of the received plaintext are reduced so much that

p_S is almost identical to p_N for $p \lesssim \frac{1}{30}$. This indicates that with the driving bit protection, the secure communication based on STCC can work as good as NNC without suffering from the bit error avalanche effect, whenever the normal communication works. To our knowledge, it is the first time that a highly secure system has such strong resistance against channel noise. In comparison, AES has much weaker resistance against channel noise. p_A is considerably larger than p_S for all range of $p \geq \frac{1}{2000}$. From the figure we anticipate that with AES secure communications with the designed bit error correction function fail at p of order 10^{-2}, at which NNC and STCC may still work. This distinction is significant in practice because wireless communications may encounter channel noise close to this range.

As an example we transmit a female voice "welcome" by applying the experiment set of Fig.3. The input signal shown in Fig.5(a) is measured at gate G3 of Fig.3, while the output signals are measured at gate G4 of Fig.3. Figures 5(b) and (c) show the results without cryptography and with channel bit error rates $p = \frac{1}{100}$ and $\frac{1}{30}$, respectively. The characteristic features of the input are kept in the output even as BER is up to $p = \frac{1}{30}$. In Figs.5(d) and (e) we do the same as (b) and (c), respectively, by including STCC cryptography and the error correction of driving bits (20 additional bits for 512 ciphertext bits). There are almost no observable deviations between STCC and NNC for both p's. In Fig.5(f) and (g) we do the same as (b) and (c), respectively, by including AES cryptography and the corresponding transmitted bit protection (8 additional bits for a block of 128 ciphertext bits). In sharp contrast, the characteristics of the input signal are essentially lost in (f) at $p = \frac{1}{100}$ and completely lost in (g) at $p = \frac{1}{30}$. From the experimental results of Figs.4 and 5 it is concluded that STCC can work much better than AES under strong channel noise.

If we set an extremely small mismatch of the encryption and decryption keys for STCC, e.g., $b_1 = a_1 + 2^{-52}$, we observe complete loss of the transmitted information (pure noise) even if the channel noise is zero ($p = 0$). This confirms the high key-sensitivity as well as high security of STCC. This sensitivity is also observed for AES experiment.

V. CONCLUSIONS

In conclusion we have suggested a cryptosystem which basically uses analytical floating-point computation and auxiliarily incorporates some algebraic operations into the basic chaotic dynamics. These combinative applications of chaotic and conventional cryptographic methods fully develop the advantages of the chaotic crytography and overcome its disadvantages, and thus achieve optimal overall cryptographic properties of high security, fast performance speed, and strong resistance against channel noise and other instabilities, which are considerably better than separative applications of both chaotic and conventional cryptosystems known so far, including AES. We have carried out an experiment practicing duplex voice secure communications in the wired PSTN. By intentionally increasing channel noise we have examined the possibility of highly secure communications in the environment of strong channel noise. It is experimentally confirmed that our chaotic cryptosystem works satisfactorily whenever normal nonsecure communication successfully works. In a range of strong channel noise ($p \approx 10^{-2}$) assumed to be encountered by some wireless communications, our system can satisfactorily perform the tasks of secure communications while AES fails to work for the same bit transmission efficiency.

This work was supported by the National Natural Science Foundation of China under 10175010 and by Nonlinear Science Project.

[1] C. E. Shannon, Bell Syst. Tech. J. 28 (1949) 656.

[2] L. M. Pecora and T. L. Carroll, Phys. Rev. Lett. vol. 64 (1990) 821 .

[3] L. M. Cuomo, and A. V. Oppenheim, Phys. Rev. Lett. 71 (1993) 65 .

[4] L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, and U. Parlitz, Int. J. Bif. and chaos 2(3) (1992) 709.

[5] L. Kocarev, and U. Parlitz, Phys. Rev. Lett.74 (1995) 5028.

[6] J. H. Xiao, G. Hu, and Zh. L. Qu, Phys. Rev. Lett. 77 (1996) 4162.

[7] D. G. Van Wiggeren and R. Roy, Science, 279(20) (1998) 1198.

[8] K. M. Short, Int. J. Bif and chaos. 4(4) (1994) 959.

[9] G. Perez, and H. Cerdeira, Phys. Rev. lett. 74 (1995) 1970.

[10] K. M. Short, and A. T. Parker, Phys. Rev. E 58 (1998) 1159.

[11] Ch. S. Zhou and C. H. Lai, Phys. Rev. E 60 (1999) 320.

[12] A. T. Parker, and K. M. Short, IEEE. Trans. Circuits Syst I. 48(5) (2001) 624.

[13] S. Papadimitriou, A. Bezerianos, and T. Bountis, IEEE Trans. on Comp. 48 (1997) 27.

[14] F. Dachselt, and W. Schwarz, IEEE trans. Circuits syst. I. 48(12), (2001) 1498.

[15] L. Kocarev, IEEE circuits syst magz. 3 (2001) 6.

[16] S. H. Wang, J. Y. Kuang, J. H. Li, Y. L. Luo, H. P. Lu, and G. Hu, Phys. Rev. E 66 (2002) 065202-1.

[17] G. N. Tang, S. H. Wang, H. P. Lu and G. Hu, Phys. Lett. A, to accept; H. P. Lu, et al, submitted

[18] J. Nechvatal, E. Barber, L. Bassham, W. Burr, M. Dworkin, J. Foti, and E. Roback, Report on the Development of the Advanced Encryption Standard (AES). Available: http://csrc.nist.gov/encryption/aes.

[19] R. E. Blahut, Theory and practice of error control codes. Addison-Wesley, NY, 1983.

[20] ITU-T Recommendation G.729, ITU-T,03/96.

Captions of Figures

Fig.1. Scheme of STCC encryption. The system is constructed with a 1D chain of length 14 and a 2D 4×4 network. In the 1D chain the six empty triangles (Δ) represent maps with the key parameters a_1, a_2, and a_3; the black triangle (▲) performs modulo and S-box operations Eq.(1b); and the seven empty circles (◯) are used for coupling the side sites of the 2D network. All the square sites (□) in the 2D network perform encryption operations Eq.(1f) simultaneously, among which the site (4,4) (black square ■) produces driving signal D_n according to Eqs.(1f) and (1a). All the solid arrows (→) denote coupling directions; K, I, and S indicate the keystream, plaintext, and ciphertext, respectively.

Fig.2. (a), (b) Error function $e(1,1;b_1)$ defined in Eq.(5) vs the decryption key parameter b_1 with different b_1 detection resolutions. $T = 10^8$. $b_2 = b_3 = a_2 = a_3$. We observe $e(1,1;b_1) = 0$ for $b_1 = a_1$, and $e(1,1;b_1) \simeq \frac{1}{3}$ whenever b_1 has any mismatch from a_1 equal to or larger than 2^{-45}. (c) $e(1,1;b_1,b_2)$ plotted in the $b_1 - b_2$ plan. $b_3 = a_3$. (d) $e(1,1;b_1,b_2,b_3)$ presented in the (b_1,b_2,b_3) space. A mesh is plotted black if $e < 0.333$, and left blank otherwise. With 2^{-45} resolution, only a single black mesh is observed at $b_1 = a_1$, $b_2 = a_2$, and $b_3 = a_3$.

Fig.3 Scheme of duplex secure speech communication experimental system. User A and user B are talking over secure telephones. User A talks through A's Microphone, which produces analog speech signal. A's Analog to Digital Converter (AD) converts the analog speech into 128Kbit/s digital speech stream (8K samples a second, 16 bits a sample). A's Source Coder compresses the digital speech into 8Kbit/s redundancy discarded speech according to a lossy speech coding standard ITU-T G.729 [20]. (Compression is needed here so that a 33.6Kbit/s channel can transmit it). A's Encryption unit encrypts the compressed speech plaintext into ciphertext by using STCC and AES systems. A's Channel Coder codes the ciphertext into an error correct code steam [19]. Then a modem modulates the digital code stream into analog signal, and send the signal to PSTN System. User B receives the transmitted signal via PSTN and the inverse processing.

Fig.4 The error bit rates p_N (squares □, for NNC), p_S (circles ◯, for STCC), and p_A (triangles △, for AES), plotted vs the error bit rate in the noisy transmission channel noise p. $p_{N,S,A}$ are computed by comparing the output signals measured at gate G2 with the input signal measured at gate G1. All plots are obtained by averaging ten measurements with each measurement taking 4Mbits. The vertical bars denote fluctuation ranges. (a) All $p_{N,S,A}$ are

measured without bit error correction. (b) $p_{S,A}$ are measured with bit error correction while p_N not. p_S is approximately equal to p_N for $p \leq \frac{1}{30}$ while $p_A > p_{N,S}$ for $p \geq \frac{1}{2000}$.

Fig.5 Analyses of the experimental data of speech signal English word ”welcome” said by a female speaker. (a) Input signal taken from gate G3 of Fig.3. (b)-(g). Received signals taken from gate G4 of Fig.3. (b), (c) Received signals with NNC and without bit error correction; (d), (e) with STCC and with bit error correction; (f), (g) with AES and with bit error correction. $p = \frac{1}{100}$ for (b), (d), (f) and $p = \frac{1}{30}$ for (c), (e), (g). In each figure the top panel shows speech signal waveform with horizontal coordinate axis representing time of 0.45 second and vertical axis the amplitude of the waveform (the largest amplitude of the input signal is normalized to one); the bottom panel presents pitch (or say, tone of speech) in $f - t$ plane with f being the pitch frequency and t time when the pitch is taken with the analysis window of 0.01 second.

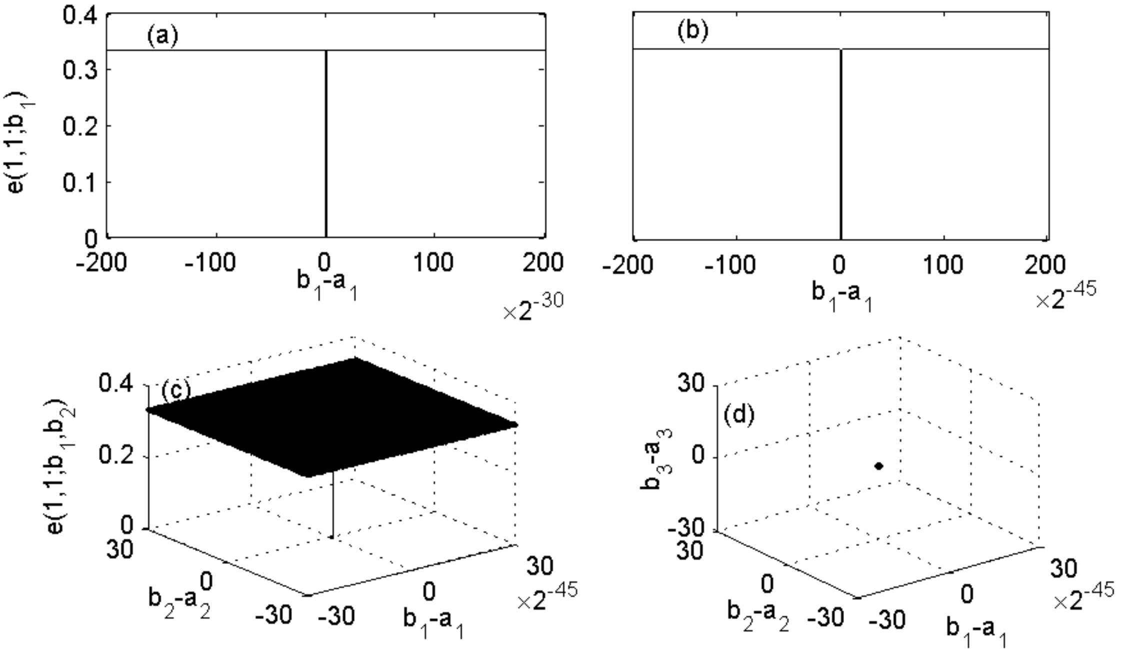
(a)
0.4
0.3
0.2
0.1
0
e(1,1;b_1)
-200
-100
0
100
200
b_1-a_1
×2^-30
(b)
-200
-100
0
100
200
b_1-a_1
×2^-45
(c)
0.4
0.2
0
e(1,1;b_1,b_2)
30
0
-30
b_2-a_2
-30
0
30
b_1-a_1
×2^-45
(d)
30
0
-30
b_3-a_3
30
0
-30
b_2-a_2
-30
0
30
b_1-a_1
×2^-45

Fig.2

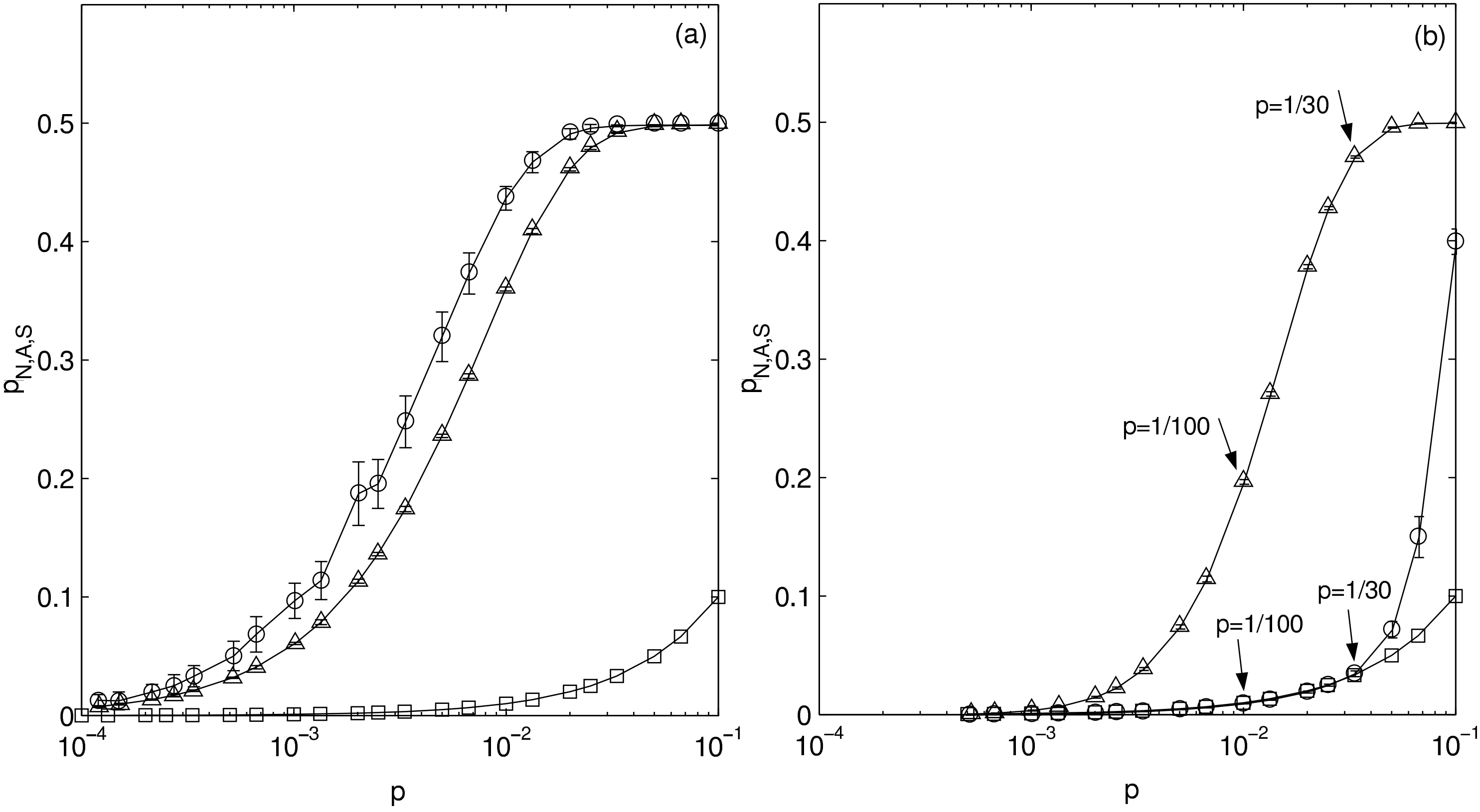
(a)
(b)
$p_{N,A,S}$
$p_{N,A,S}$
0.5
0.4
0.3
0.2
0.1
0
10^{-4}
10^{-3}
10^{-2}
10^{-1}
p
p
p=1/30
p=1/100
p=1/100
p=1/30

Fig 4